Feinstein Testifies on Recent Data Breaches and Her Identity Theft Notification Bill at Judiciary Committee Hearing

April 13, 2005

Washington, DC *– At a Senate Judiciary Committee today, U.S. Senator Dianne Feinstein (D-Calif.) called on the Senate to approve legislation that she has sponsored to ensure that consumers are notified when their personal information is compromised in such a breach.*

Senator Feinstein's legislation requires a business or government entity to notify an individual in writing or email when it is believed that personal information – such as a Social Security number, driver's license or state identification number, or credit card or bank account information – has been compromised. Only two exceptions to notification exist -- upon the written request of law enforcement for purposes of a criminal investigation, and for national security purposes.

The following is the prepared text of her statement:

"Thank you Chairman Specter and Senator Leahy for giving me the opportunity today to testify on behalf of the 'Notification of Risk to Personal Data Act of 2005'.

I strongly believe that the notification bill that I re-introduced Monday afternoon (S. 751) – and which is a strengthened version of S. 115 that I introduced in January – is necessary to help protect Americans from the vast and growing crime of identity theft. This bill will ensure that Americans are notified when their most sensitive personal information – their Social Security Number, their driver's license or state identification number, their bank account and credit card information – is part of a data breach putting them at risk of identity theft.

Just yesterday, we learned that LexisNexis underreported the number of individuals whose personal information may have been stolen in March of this year. Instead of 32,000 individuals being potentially affected by the breach at its newly acquired Seisint unit, 310,000 people nationwide may have been affected and their personal data stolen.

But since February 2004 alone, there have been at least 12 major breaches of databases which has placed 10.7 million people in jeopardy of identity theft. These are just the cases that we know about. Who knows the impact of the cases that we don't. And there were 9.3 million reported cases of identity theft last year alone, including 1 million in California.

So what can we do? We urgently need a strong national standard that says whenever a data system is breached, everyone who is at risk of identity theft must be notified.

Here's what the bill does: It requires a business or government entity to notify an individual in writing or email when it is believed that personal information – such as a Social Security number, driver's license, or credit card number – has been compromised.

Only two exceptions to notification exist. First, upon the written request of law enforcement for purposes of a criminal investigation; and second, for national security purposes.

This bill is based on the ground-breaking California law which is the first and only State law requiring notification of individuals. The California law really opened our eyes to the problem. Without it, we probably wouldn't have heard about half of the cases I mentioned before.

But in fact, the legislation I'm introducing today is much stronger than the California law. **Here's how:**

- It covers both electronic and non-electronic data – as well as encrypted and non-encrypted data. The California law only includes unencrypted, electronic data.

- It allows individuals to put a 7-year fraud alert on their credit report. The California law doesn't address fraud alerts.

- It doesn't include a major loophole allowing companies to follow weaker notification requirements – as the California law does.

- It lays out specific requirements for what must be included in notices, including:

    - a description of the data that may have been compromised;
    - a toll-free free number to learn what information and which individuals have been put at risk;
    - and the numbers and addresses for the three major credit reporting agencies.

- By contrast, California law is silent on what should be in notices.

- It has tougher civil penalties -- $1,000 per individual they failed to notify or not more than $50,000 per day while the failure to notify continues or existed. In California, a victim may bring a civil action to recover damages or the company may be enjoined from further violations.

- And most importantly, it sets a national standard – so that individuals in Iowa, Oklahoma, and Maine have the same protections as consumers in California.

- The law would be enforced by the Federal Trade Commission or other relevant regulator, or by a State attorney general who could file a civil suit.

And because the bill is stronger than California law, leading privacy groups – including Consumers Union and the Privacy Right's Clearinghouse – have endorsed this legislation.

You can't tell the true impact of identity theft by looking at the numbers. You see it in the stories of the victims. Let me tell you how identity theft works.

While Rebecca Williams was living in San Diego in April 2000, a thief was using her Social Security number, her birthdate, and her name to establish a parallel identity thousands of miles away in the Chicago area.

The thief opened a household, obtained a driver's license, and signed up for credit cards in her name. The thief even tried to use her identity to purchase a car. In all, the thief used Ms. William's identity to open more than 30 accounts, accruing tens of thousands of dollars worth of goods and services. Sometimes accounts were opened despite the fact that fraud alerts had been issued.

Ms. Williams says that restoring her identity is "like a full-time job" and estimates that she has spent the equivalent of 8-hours a day for three full months working with credit bureaus, credit card companies, and various government agencies trying to put her life back together.

But five years later, Ms. Williams still has not fully restored her identity – she faces two civil judgments for unpaid rent for apartments she never lived in, she faces higher interest rates for loans and credit cards, and she lives in fear that the thief, who has never been caught, will once again use her identity as a source of income.

This is not an isolated incident. This is happening in every community across the country. Sometimes it is an individual acting alone. Other times it is part of an identity theft ring. But in every case, there is a victim who has been violated in an extremely personal way.

I strongly believe individuals have a right to be notified when their most sensitive information is compromised – because it is truly their information. This bill will give all Americans more control and confidence about the safety of their sensitive personal information.

It will help combat the growing scourge of identity theft. And if an identity theft does occur, it will give individuals the ability to protect themselves from further fraud. I look forward to working with my colleagues to pass this critically important legislation.

Thank you, Mr. Chairman and Senator Leahy."

###